BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 31-702

18 FEBRUARY 1994

Security

SYSTEM SECURITY ENGINEERING

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the SAF/AAD WWW site at: http://afpubs.hq.af.mil. If you lack access, contact your Publishing Distribution Office (PDO).

OPR: HQ AFMC/SPX (Lt Col William C. Conrad)
Supersedes AFR 800-23, 23 May 1986.

Certified by: HQ USAF/SP (Brig Gen Stephen C. Mannell)
Pages: 10
Distribution: F

This instruction implements AFPD 31-7, *Acquisition Security*, and DoD Instruction 5000.2 , *Defense Acquisition Management Policies and Procedures,* February 23, 1991, with Change 1, by integrating various security disciplines to give program managers and weapons system users a method they can use to evaluate threats and plan security countermeasures.

SUMMARY OF REVISIONS

This is the initial publication of AFI 31-702. It outlines the phase-by-phase actions you take for system security engineering management when acquiring or purchasing weapons; clarifies the current acquisition process; outlines the requirements for acquisition security training; and deletes the portion pertaining to "Relationship to the Air force Physical Security Program."

1. Purpose. The purpose of the System Security Engineering Program is to identify the methods and actions needed to minimize or contain system or component vulnerabilities.

1.1. Program managers must identify significant vulnerabilities before Acquisition Milestone I and reduce the likelihood of damage, compromise, or destruction to the system.

NOTE:

System Security Engineering does *not* deal with specific weapons capabilities to counter combat threats.

1.2. Program managers establish procedures to:

- Identify all security requirements and integrate them into a single program.
- Tailor individual security disciplines to program development efforts as inexpensively as possible.

- Organize efforts to effectively ensure security and engineering integration.
- Identify physical, electronic, and intelligence threats that you can neutralize or minimize through security engineering design and countermeasures.
- Identify the actions you need to take to minimize or contain system or component vulnerabilities.
- Lower security costs over the life of the system, and improve overall survival rates of a system or component.

2. Responsibilities:

2.1. The Chief of Security Police (HQ USAF/SP) 1340 Air Force Pentagon, Washington DC 20330-1340:

- Includes system security engineering requirements in system requirements documents; for example, mission need statements (MNS), operational requirement documents (ORD), program management directives (PMD), and other applicable documents.
- Coordinates with program element monitors on security engineering requirements during the acquisition process.
- Guides and assists major commands (MAJCOM) and field operating agency staffs in meeting Air Force policy directive requirements for acquisition security.

2.2. The DCS Command, Control, Communications and Computers (HQ USAF/SC), 1250 Air Force Pentagon, Washington DC 20330-1250, establishes guidelines on information systems security, communications security, and compromising emanations (TEMPEST) policy.

2.3. Headquarters, 497th Intelligence Group, Directorate of Security and Communications (HQ 497th IG/INS), 211 Brookley Avenue, Suite 200, Bolling AFB DC 20332-5108, establishes guidelines on security for Sensitive Compartmented Information.

2.4. The Chief, Foreign Disclosure Policy Branch, Deputy Under Secretary of the Air Force for International Affairs (SAF/IADP), 1010 Air Force Pentagon, Washington DC 20330-1010, establishes foreign disclosure guidelines for System Security Engineering Management Plans.

2.5. DCS Plans and Operations, Technical Plans Division (HQ USAF/XOXT), 1480 Air Force Pentagon, Washington DC 20330-1480, establishes Operations Security (OPSEC) guidelines.

2.6. Headquarters, Air Force Office of Investigations (HQ AFOSI/IOC), 226 Duncan Avenue, Bolling AFB DC 20332-0001, supports counterintelligence efforts. AFOSI:

- Collects, analyzes, evaluates, and disseminates counterintelligence information on security threats to US Air Force and Department of Defense operations and resources.
- Provides, to the appropriate offices, program and system threat and vulnerability information to develop system security plans and countermeasures.
- Describes and analyzes intelligence and security threat data, helps develop scenarios, and conducts interactive threat and vulnerability analysis.

2.7. Acquisition Management and Policy Division, Deputy Assistant Secretary of the Air Force for Management, Policy, and Program Integration, (SAF/AQXA), 1060 Air Force Pentagon, Washington

DC 20330-1060, includes Systems Security Engineering in all program management directives (PMD).

2.8. Headquarters Air Force Materiel Command, Office of Security Police (HQ AFMC/SP), 4225 Logistics Avenue, Suite 21, Wright-Patterson Air Force Base OH 45433-5760:

- Directs an Air Force training program for security personnel who support the acquisition process.
- Helps MAJCOM staffs identify security requirements and resolve security issues.
- Acts as office of primary responsibility (OPR) for Military Standard (MIL-STD) 1785, *System Security Engineering Management*.
- Acts as OPR for security enrollment in the Acquisition Professional Development Program (APDP).

2.9. The Using Command Security Police Staff:

- Helps users write requirements documents to include clear, accurate security requirements.
- Establishes security requirements during MNS and ORD development.
- Develops a system security concept that includes acquisition security as defined in AFPD 31-7.
- Takes charge of system security engineering and related issues.
- Coordinates with the supporting command or agency security requirements for systems scheduled to undergo depot maintenance.
- Participates in major system (Acquisition Category [ACAT] I/II) system security working group (SSWG) meetings, and when requested by the program office, attends SSWG meetings for other programs.
- Ensures that Air Force labs meet security engineering requirements before formal establishment of a program in research and development projects.

2.10. The Implementing Command Security Police Staff:

- Develops security countermeasures based on threat analyses provided by AFOSI and other sources.
- If implementing and supporting commands differ, coordinates with supporting command to ensure that adequate, continuous security arrangements exist.
- Supports the system security working group for major systems (ACAT I/II) and other systems, as required by the program office.
- Assesses the impact on security of system engineering change proposals, deviations, and waivers through the life of the system.

2.11. The Supporting Command Security Police Staff Responsibilities:

- Establishes system security engineering support to ensure security for systems that are undergoing maintenance or modification.
- Assesses the impact on security of system engineering change proposals, deviations, and waivers.
- Participates on the system security working group, as required by the program office.

2.12. The Participating Command Security Police Staff:

- Coordinates any efforts that may impact the system's security with the implementing and operating commands.
- Assists in security planning, when requested.

3. Procedures:

3.1. The system security engineering manager's first direct involvement usually comes during development of the ORD. You must include the operational command that develops the ORD and security engineering requirements in the MAJCOM ORD development and coordination process.

3.2. Plan for security from the beginning. Advance planning cuts costs by eliminating the need to retrofit security into an existing system, or requiring the use of manpower-intensive security where a less expensive solution was possible.

3.3. Involve the operating MAJCOM-level security personnel to help include security requirements in the product.

4. Training Requirements:

4.1. Individuals who support the acquisition management process must receive acquisition training. Minimally, this includes the introductory course in systems acquisition.

4.2. Individuals in the APDP must meet training requirements as soon as possible after they are assigned to that position, but no later than the maximum amount of time allowed for APDP certification. See DoD 5000.52-M, *Career Development Program for Acquisition Personnel*, November 1991, for specific requirements concerning APDP certification.

4.3. Personnel performing acquisition security tasks must receive training in Program Protection Planning, System Security Engineering, and Product Security.

5. Security In Each Acquisition Phase. Following is an overview of what program managers need to do to ensure security throughout the acquisition process.

5.1. Phase 0, Concept Exploration and Definition:

- Program Protection Plan (PPP) managers provide a PPP to the Defense Acquisition Board or Designated Acquisition Commander by Milestone I.
- The System Security Management Plan (SSMP) defines the organization, management, and implementation approach for systems security. The SSMP must integrate secure systems capabilities and provide a single process for security risk management.
- Security threat analysis evaluates threats to the system. The security threat analysis describes the potential threat capability of adversaries and possible political, economic, and hostile adversary motives.
- System vulnerability assessment determines, based on the security threat analysis, how sensitive or critical the system components, procedures, and support elements are in their operational environment.
- Security test and evaluation defines test and evaluation procedures to verify multidisciplinary security system requirements. It also evaluates the results and notes any deficiencies.

5.2. Phase I, Demonstration and Validation:

- Assesses alternate security systems for suitability and cost comparison.
- Since security test and evaluation processes are critical during this phase, identifies alternative methods where necessary.

5.3. Phase II, Engineering and Manufacturing Development:

- Helps program managers reduce security costs by applying the results of the security test and evaluation phase to risk management.
- Reduces potential threats, noted in Phase I, to actual threats identified through security test and evaluation, and additional threat analyses.
- Commits system resources to develop countermeasures for the actual threats.
- Develops system performance requirements for contract specifications in coordination with the user or the user's representative.

5.4. Phase III, Production and Deployment:

- Applies security testing criteria developed in prior phases to ensure applicability and validity.
- Implements product security requirements.

5.5. Phase IV, Operations and Support:

- Checks existing systems in the field for the effects of aging on security systems.
- Modifies security systems, when appropriate, to extend the life of the system.

6. Systems Security Engineering Management Tasks. System security engineering management tasks are tailored to program needs. Systems security engineering management applies scientific and engineering principles to identify and reduce security vulnerabilities.

7. MIL-STD 1785. Base systems security engineering management on MIL-STD 1785, which sets the standard for contents and procedures of a contract or government systems security engineering management program.

8. SSMP. SSMP formally documents security tasks to meet system security requirements. It must include the following elements:

- Organizational responsibilities.
- Methods of accomplishment.
- Milestones.
- Depth of effort.
- Integration with other program engineering.
- Design and management activities.
- Related systems.

9. Threat Definition:

9.1. Defining the threat is fundamental to systems security. The intelligence organization with which you work, or AFOSI provides specialized acquisition security threat information.

9.2. The effectiveness of a security system against a threat depends on how well you develop adversary mission objectives and scenarios for the system. The threat definition provides a preliminary estimate of the effect of the threat on each system or design alternative. Validate system security criteria using the threat environment, since it represents the best quantitative estimate available.

10. Security Threat Analysis. The security threat analysis is an annex to the SSMP. It correlates potential adversary and threat characteristics, postulated capabilities, and plausible political, economic and adversary incentives, both during peacetime, and during periods of increased international or domestic tension.

11. System Vulnerability Analysis. Base the vulnerability analysis on the security threat analysis, and address all system elements. The vulnerability analysis compares threat capabilities, characteristics and incentives to system components, operational procedures, logistics concepts, and support equipment. It identifies critical system components, procedures, and support elements based on their value to the adversary.

12. System Security Concept. Base the system security concept on the system vulnerability analysis. This will help identify security concepts and requirements you need to counteract system vulnerabilities.

13. Request for Proposal (RFP) and Statement of Work (SOW):

13.1. The government uses the RFP to negotiate acquisitions. The RFP specifies government requirements and solicits proposals to satisfy those requirements.

13.2. The SOW clearly specifies required development or production work for deliverable goods or services from a contractor.

13.3. The RFP and SOW must include specific security requirements that the contractor must satisfy.

13.4. Include the using command in the development of the RFP and SOW. Although the security engineering process does not specifically include the RFP and SOW, the system security engineering manager must use these documents to establish requirements that begin the process.

14. SSWG:

14.1. SSWG is a working forum of experts who support security engineering and concept development tasks and work closely with the program manager to run the system security engineering program. The size and nature of the program and system being developed dictate the size and makeup of the SSWG. Members of the SSWG assist in the preparation of the following documents and material:

- Security Threat Analysis.
- Systems Vulnerability Analysis.
- System Security Concept.
- System Security Management Plan.

14.2. The implementing command forms the SSWG using a charter that specifies the purpose, membership, procedures, functions, tasks, and administration requirements of the organization (see **Attachment 1** for a sample charter).

14.3. A senior program official, such as the system program director, usually chairs the group.

14.4. Do not limit membership arbitrarily. Include representatives from any organization that can directly contribute to the system security development. Consider including non-Air Force organizations and agencies that create military component or national-level policies affecting system security.

15. Acronyms Used:

ACAT—Acquisition Category

AFOSI—Air Force Office of SpecialInvestigations

APDP—Acquisition ProfessionalDevelopment Program

MAJCOM—Major Command

MNS—Mission Needs Statement

OPR—Office of PrimaryResponsibility

OPSEC—Operations Security

ORD—Operational Requirements Documents

PMD—Program ManagementDirective

PPP—Program Protection Plan

RFP—Request for Proposal

SOW—Statement of Work

SSMP—System Security Management Plan

SSWG—System Security Working Group

TEMPEST—Compromising Emanations

STEPHEN C. MANNELL, Brig General, USAF
Chief of Security Police

Attachment 1

EXAMPLE OF SSWG CHARTER (PROGRAM NAME)
SYSTEM SECURITY WORKING GROUP CHARTER

A1.1. Purpose of the SSWG. The SSWG formulates and recommends (program name) system security engineering policy and procedures concerning ground threats and system vulnerabilities.

A1.1.1. The SSWG reviews requirements for the following:

- Physical security.
- Information systems security.
- Communications security.
- TEMPEST.
- Personnel security.
- Industrial security.
- Information security.
- Security education.
- OPSEC.
- Technology control.

A1.1.2. The SSWG reviews contractor system security engineering performance, identifies problems, and recommends solutions. It also addresses survivability, basing, and systems operation issues, and reviews candidate safeguards.

A1.2. SSWG Objectives:

- Serve as the focal point for identification, discussion, and resolution of all program security-related issues.
- Make sure that the using Air Force MAJCOM can accept the (*system name*) into a secure environment that meets its security requirements.
- Assess existing, or develop new, protection policies, procedures, and certification or accreditation criteria, if necessary, to integrate weapon system.
- Manage the security test and evaluation to support (*system name*) certification and accreditation.
- Review and provide security inputs to plans (such as the Test and Evaluation Master Plan and the Integrated Logistics Support Plan), training, and maintenance to meet (*system name*) security requirement.
- Ensure the orderly transition of security requirements to the operational Air Force.

A1.3. SSWG Membership:

A1.3.1. Base the (program name) SSWG permanent membership on program needs; and augment the membership as required.

A1.3.2. Any permanent group member can request that you add additional members to the group as long as the majority of the current membership supports the addition.

A1.3.3. The SSWG membership should include, but not be limited to, representatives from the following areas:

- Program Office.
- Program Engineer.
- Program Scientist.
- Information Security.
- Industrial Security.
- Personnel Security.
- Physical Security.
- Systems Security Engineering.
- Foreign Disclosure Office.
- Special Security Office.
- Communications Security.
- TEMPEST.
- Information Systems Security.
- Counterintelligence.
- OPSEC.
- Special Access Program Representative (where applicable).
- Science and Technology.

A1.3.4. All members must meet the basic program requirements for security clearances and program access.

NOTE:

Do not arbitrarily limit membership. Base membership on actual program needs. You can add additional members as you need them to meet specific requirements, for example, you can ask the Special Security Officer to serve when the system will be using, storing, transporting, or processing sensitive compartmented information.

A1.4. SSWG Organization:

A1.4.1. The System Program Director , or designated representative, chairs the SSWG. The chairperson approves membership, sets SSWG direction, and recommends/closes action items.

A1.4.2. The (program name) The systems security engineering manager serves as the group's recorder.

NOTE:

Depending on the size and acquisition category of the program, you may find it useful to create SSWG subworking groups, particularly for programs using Integrated Product Teams. In that case, you can expand this paragraph to describe such organization.

A1.5. Functions and Tasks of the SSWG:

- Identify, define, and document, system security requirements for the life of the system from (*program phase*) through disposal in the SSMP.
- Review (*program name and system name*) ground threat and vulnerabilities analyses.
- Identify new or changing ground threats to (*system name*).
- Review system security concepts and designs that are being considered for integration into (*system name*).
- Recommend personnel security criteria and procedures.
- Recommend logistics security procedures.

NOTE:

The above list is an example only. Each program's actual requirements will vary, depending on program needs.

A1.6. SSWG Administration:

A1.6.1. The chairperson sets the time and place for meetings. Hold meetings semiannually, unless system requirements dictate otherwise. Notify members in writing, and provide them with an agenda. Formulate tentative agendas for subsequent meetings at the end of each meeting.

A1.6.2. Have the systems security manager, or whoever the chairperson appoints, take minutes at each meeting. Distribute the minutes within 15 days after the meeting.

A1.6.3. Observe all applicable security regulations and policies pertaining to the program.

A1.6.4. All member organizations provide their own administrative, travel and per diem funds in support of working group activities from their own budgets.

A1.6.5. Members can recommend changes to this charter in writing to the chairperson. All changes must have the agreement of the full membership. Review the charter annually for accuracy and currency. You must get the system program director to approve the charter.

NOTE:

You can include attachments appropriate for the program. For example, you can attach a list of permanent members and organizational outlines.